REMARKS

Claims 46-72 were pending in the application. Claims 1-45 and 73-124 are withdrawn from consideration. Claims 1-45 and 73-124 have been canceled. Of the pending claims, Claim 46 is an independent claim. Claims 125-129 are newly added.

Claims 48, 51-53, and 64 are objected to under 37 C.F.R. 1.75(c) as being of improper dependent form for failing to further limit the subject matter of the previous claim. Claims 46-72 are rejected under 35 U.S.C. 101 as lacking patentable utility. Claims 49, 50, 55 and 60-64 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Claims 48, 50-53, 60-64 and 72 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 49, 50 and 67 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. Claims 46-53, 55, 56, 65, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Child et al. (U.S. Patent No. 6,341,352) in view of Swift et al. (U.S. Patent No. 5,719, 941). Claims 54, 57-59, 60-64, and 69-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Child in view of Swift as applied to claims 46 and 47 above and in further view of Kadooka (U.S. Patent No. 5,606,663). These rejections are respectfully traversed and reconsideration is requested.

Regarding Objections under 37 C.F.R. 1.75(c)

Claims 48, 51-53, and 64 are objected to under 37 C.F.R. 1.75(c) as being of improper dependent form for failing to further limit the subject matter of the previous claim.

In response, claim 48 has been amended to clarify that claim 48 further limits the step of verifying the continuation message recited in dependent claim 47.

Claim 51 has been rewritten in independent form including all the limitations of claim 46. Claims 52 and 53 depend from claim 51 and further limit the subject matter of claim 51. Claim 64 has been amended to clarify that claim 64 further limits the step of checking recited in claim 60.

Removal of the objections to claims 48, 51-53, and 64 under 37 C.F.R 1.75(c) and acceptance of claims 48, 51-52 and 64 is respectfully requested.

Regarding Rejections under 35 U.S.C. 101

Claims 46-72 are rejected under 35 U.S.C. 101 as lacking patentable utility. The applicants' disclosed invention prevents piracy of software while protecting the privacy of the user of the software by verifying that a tag table storing tags (licenses) associated with instances of software installed on the user device is only stored in one user device. Messages are exchanged between a supervising program (trusted agent) on the user device and a guardian center with hash function values of a tag table storing a tag for a copy of software. Previously sent hash values are stored in the guardian center and compared. In response, claim 46 has been amended to recite "to detect use of an infringing copy of software on the user device by detecting tag tables on different user devices having the same tag table identifier value". This use is described in the applicants' specification as originally filed. (*See* Page 40 lines 11-16; Page 18, lines 6-9; Page 19, lines 22-29; Page 55, line 26 – Page 55, line 4; Page 56, lines 10-24.) Claims 47-50 and 52-72 are dependent claims that depend directly or indirectly on claim 46 and thus include this limitation. Claim 51 rewritten in independent form also recites this use.

Removal of the rejections to claims 46-72 under 35 U.S.C. 101 and acceptance of claims 46-72 is respectfully requested.

Regarding Rejections under 35 U.S.C. 112, first paragraph

Claims 49, 50, 55, 60-64 and 67 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

Without acquiescing to the rejection, claim 49 has been canceled. Claim 50 has been amended to clarify that the guardian center re-sends the continuation message, in response to the supervising program resending the call-up message. (*See* Applicant's specification Page 42, lines 3-17.) Claim 55 has been amended to clarify that the hash function values in the continuation message are replaced. (*See* Applicants' specification, Page 41, lines 25-26.) Claims 60-64 are directed to a user device having a plurality of tag tables. (*See* Applicants' specification Page 43, line 17- Page 45, line 24.) Claim 67 has been amended to clarify that the guardian

center computes a hash function value of superfingerprints previously sent to the user device and superfingerprints sent in the continuation message. (*See* Applicants' specification Page 54, line 16- Page 55, line 9.)

Removal of the rejections to claims 49, 50, 55, 60-64 and 67 under 35 U.S.C. 112, first paragraph and acceptance of claims 49, 50, 55, 60-64 and 67 is respectfully requested.

Regarding Rejections under 35 U.S.C. 112, second paragraph

Claims 48, 50-53, 60-64 and 72 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 49, 50 and 67 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps.

In response, claim 48 has been amended to clarify that "said verification" refers to the verification step of claim 47. Claim 49 has been canceled. Claim 50 has been amended to clarify that the guardian center re-sends the continuation message, in response to the supervising program resending the call-up message, that is, if the call-up is not completed because the supervising program in the user device did not receive the continuation message sent by the guardian center. (*See* Page 42, lines 3-17; Fig. 11B, steps 1511, 1510.) Claims 51-53

Claim 60 has been amended to provide antecedent basis for "hash function values".

Claim 60 has also been amended to clarify that user device descriptive values are stored in a tag table. (*See* Applicants' specification Page 39, lines 1-20.) Claim 64 has been amended to provide antecedent basis for "tag tables". Claim 67 has been amended to clarify that superfingerprints are stored in the user device and to add additional steps. Claim 68 has been amended to provide antecedent basis for "user device time". Claim 72 has been amended to provide antecedent basis for "total usage".

Removal of the rejections to claims 48, 49, 50-53, 60-64, 67 and 72 under 35 U.S.C. 112, first paragraph and acceptance of claims 48, 49, 50-53, 60-64, 67 and 72 is respectfully requested.

Regarding Rejections under 35 U.S.C. 103(a)

Claims 46-53, 55, 56, 65, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Child et al. (U.S. Patent No. 6,341,352) in view of Swift et al. (U.S. Patent No. 5,719, 941). Claims 54, 57-59, 60-64, and 69-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Child in view of Swift as applied to claims 46 and 47 above and in further view of Kadooka (U.S. Patent No. 5,606,663).

Before addressing the rejection there is set forth a brief discussion of the applicants disclosed embodiments of the invention. The applicants disclosed invention is directed to a non-voluntary, privacy-preserving method for protecting intellectual property rights of vendors and owners of software against piracy by a user on a user device. A copy of the software is stored on the user device with a tag incorporating a tag table identifier. The tag table identifier contains no information such as a device number which could identify the user or the device and would thus impinge on the user's privacy with respect to which software is used. To prevent the situation that after purchase by one user, several user devices share the same tag and simultaneously use copies of the same software, the claimed method ensures that the same tag table identifier cannot be validly present at the same time on a multiplicity of user devices. This is performed by sending call-up messages from a supervising program on a user device to a guardian center, and of sending continuation messages from the guardian center to the user device. *(See* Claim 46)

The supervising program computes hash functions values of the tag table, and sends just the hash function values in the call-up message to the guardian center in order to conceal from the guardian center the names of the software stored in the tag table, thus preserving the user's privacy. The guardian center records only tag table identifiers which, if so desired by the user, cannot be linked to him if he performs anonymous call-ups.

Turning to the cited art, Child is directed to security policy, for example, managing password expiration in a secure distributed file system. Upon receiving a request from a user for a file and detecting that the user's password that allows the user to access the file system has expired, a change password utility is automatically invoked to allow the user to change the password. After the password has been changed, the original request continues.

Cited art Swift is also directed to security policy in a client-server environment. A password is encrypted so that it can be securely transmitted over the network to the server.

Cited art Kadooka is also directed to security policy in a client-server environment. In the system discussed by Kadooka user passwords are assigned an expiration time.

Child's discussion of a method for changing a password and Swift's discussion of a password changing method that is secure (through the use of hashing) separately or in combination do not teach or suggest the Applicants' disclosed method for preventing piracy of software stored in a user device by detecting tag tables of different user devices having the same tag table identifier. Child and Swift separately or in combination do not prevent more than one user using the same password to access the file system. In the systems discussed by Child and Swift files are stored in the server and multiple users are given permission to use the files. There is no suggestion of preventing more than one user from using the files. Furthermore there is no suggestion of the need to prevent more than one user from using the same password. In the client-server models described by Childs and Swift, each remotely stored file is shared by a plurality of users. In contrast, in the applicants' claimed invention each locally stored software is usable only by one user device through the use of a tag associated with the software, and the guardian center together with the supervising program in the user device monitor the tag table identifier through the use of call-up and continuation messages to ensure that the tags associated with the tag table are not being used by another user device.

Neither Child or Swift or Kadooka separately or in combination teach or suggest the applicants' claimed "computing, by a supervising program within said user device, a first hash function value of a tag table stored in the user device, said tag table including a tag for a copy of software stored in the user device, said tag comprising a tag table identifier value and a hash function value of a portion of said copy of software". None of the cited art is even directed to the applicants' claimed method for supervising usage of software that is stored in a user device. The cited art merely discusses managing access to remote files under control of the user. The files in the remote system are shared by a plurality of users through the use of a password that is assigned to a user in order to allow the user to access the files stored on the remote system.

In contrast, the applicants' claimed invention is directed to supervising use of a locally stored copy of software to ensure that the copy of software is not shared by others. The copy of

software is stored in the user device and permission to access and use the software is dependent on a tag (license) that the user device has obtained to use the software. For example, if a user device stores a copy of software but has not purchased the software (for example, if the software is preloaded by a vendor but without permission to use), no tag is stored in the tag table for the software and the user does not have permission to access and use the software.

Child does not teach or suggest the Applicants' claimed "tag table". The tag table stored in the user device includes a tag for a copy of software stored in the user device. The tag includes an identifier value of the tag table and a hash function value of a portion of the copy of software. In contrast, Child merely discusses a password that is associated with a user identifier and stored in a remote system.

Child does not teach or suggest the Applicants' claimed "call-up" message. The call-up message is sent from the user device to a guardian center and includes hash function values of the tag table and the identifier value of the tag table that is stored in the tag in the tag table associated with the copy of software. Child's discussion of a change security policy dialog with the user does not teach or suggest the applicants' claimed "call-up message". Child discusses two basic routes through the protocol: user submits request, server determines there is no need for a password change and so executes the transaction; or user submits request, server sets up dialogue for password update, user sets new password and responds, then server executes the transaction. (*See* Child col. 7, line 51.) In contrast, the applicants' disclosed invention entails no dialog with the user nor is there a change in security policy. The transaction is a one request-response interaction: the supervising program within the user device sends a call up message comprising a tag table identifier, a first hash function value of a tag table, and a second hash function value of the tag table sent in the previous call-up message. The guardian center responds with a continuation message. Every interaction entails these two messages (call up message and continuation message) (*See* Fig. 1, 102, 104.). There is no dialog because the user need not, in fact should not, be involved. In Child, the user voluntarily changes password and can choose a password. In the Applicants' invention, the supervising program sends the call up message, if the user were involved, then the user could manipulate the hash function values and unlawfully share a tag table with other user devices allowing the same copy of software to be shared with other user devices.

Swift does not teach or suggest the Applicants' claimed "first hash function value of a tag table". Swift merely discusses the use of hashing to protect a password selected by the user. There is no discussion of a tag table storing tags associated with a copy of software. In the Applicants' claimed invention, the supervising program within said user device computes a "first hash function value of a tag table". It is the computed first hash function value that is sent in a call-up message to a guardian center. The use of a hash function value of a tag table preserves the privacy of the user with respect to the identity of the software that is stored in the user device. The hash function value of the tag table represents the tags (licenses) possessed by the user device that are stored in the tag table without revealing the identity of the software stored in the user device to the Guardian Center.

The Examiner has taken Official Notice that the storing of correspondence or requests, as well as the time and date of said correspondence or request, regarding user personal information, between a user and a service provider is old and well-known to those of ordinary skill of customer service. The Applicants respectfully traverse the Examiner's assertion of Official Notice. The Applicants' disclosed invention is not directed to customer service and does not store correspondence or requests, regarding user personal information, between a user and a service provider. Instead, the Applicants' claimed method for supervising usage of software stored in a user device involves a series of messages between a supervising program (not a user) within the user device and a guardian center. The supervising program within the user device computes a hash function value of a tag table to preserve the privacy of the user; that is, the identity of the software that is stored on the user device is not disclosed to the guardian center nor is the identity of the user. Personal information about the user is not transmitted. The supervising program provides the hash function value of the tag table to the guardian center, so that the guardian center can verify that the hash function value of the tag table sent in the previous call-up message is a most recently stored value in a list of hash function values stored by the guardian center. The purpose of verifying such an association is to detect and halt the duplication of a tag table on several user devices.

The Examiner has also taken Official Notice that the use of digital signatures (e.g. superfingerprints) for authenticating communications is old and well-known. The Applicant respectfully traverses the Examiner's assertion of Official Notice. Although, as suggested by the

Office, the use of digital signatures to prove that a message has been sent from a particular device, may be known, the use of digital signatures does not suggest the applicants' disclosed "superfingerprints". The Applicants disclosed superfingerprints are used to detect which software is running on a user device in contrast to digital signatures that are used to authenticate the source of a message.

Child does not teach or suggest the applicants' claimed "sending, by said guardian center, a continuation message to said supervising program, said continuation message comprising a portion of said call-up message". In the password dialog discussed by Child, the new password is not sent back to the user device. There is no need to return the password in a password changing application. In the applicants' disclosed invention, portions of the call-up message are sent back from the guardian center to the user device for later verification by the supervising program. (*See* claim 47.)

Swift is cited for its discussion of an encrypted password. The combination of Child and Swift merely discusses a secure method for changing a password. Swift does not teach or suggest the applicants' claimed "tag table" or "tag table identifier". Only the passwords that are stored in the remote system (server) are encrypted. The combination of Swift and Child merely discusses use of a password dialog to change an encrypted password which does not teach or suggest the applicants' claimed invention.

Regarding the obviousness rejection the Office has further cited In re Japikse, 86 USPQ 70 in support of a holding that rearranging parts of an invention involves only routine skill. However, in view of the fact that the Office has not even shown all of the claimed elements, this rejection is moot.

In addition, there is also a lack of any teaching, motivation, or suggestion to change the location of components. The mere fact that parts of an invention can be re-arranged is not by itself sufficient to support a finding of obviousness. The reference must provide a motivation or reason to make the change. There is no suggestion in Child or Swift of storing a password in a client instead of in a server. (*See* Ex parte Chicago Rawhide Mfg. Co., 223 USPQ 351, 353 (Bd. Pat. App. & Inter. 1984.)

Claims 54, 57-59, 60-64 and 69-70 are dependent claims that depend directly or indirectly on claim 47 which has already been shown to be non-obvious over the cited art.

Furthermore, these claims include additional features which are not suggested by the cited art. For example, Kadooka does not suggest "storing user descriptive values in said tag table" as claimed by the applicants in claim 60. Additionally, Kadooka does not suggest "storing a plurality of tag tables. Kadooka does not even suggest storing a single tag table. In contrast, Kadooka merely discusses initiating a change password utility at a periodic time interval. The Office has cited In re Harza, 124 USPQ 378 in support of a holding that mere duplication of parts has no patentable significance unless a new and unexpected result is produced. However, in view of the fact that the Office has not even shown all of the claimed elements, this rejection is moot.

Claims 47-48 and 50-72 are dependent claims that are directly or indirectly dependent on claim 46 that is not obvious over the cited art. Thus, the cited art, separately or in combination, does not teach or suggest the Applicants' claimed invention.

Accordingly, the present invention as now claimed is not believed to be anticipated by or made obvious from the cited art or any of the prior art. Removal of the rejections under 35 U.S.C. 103(a) and acceptance of Claims 46-48 and 50-72 is respectfully requested.

Regarding new Claims 126-129

Support for newly added Claim 125 is found at least in Applicants' claims 46 and 66 as originally filed. Support for newly added Claim 126 is found at least on Page 39, line 26 – Page 40, line 4. Support for newly added Claim 127 is found at least on Page 55, line 26 – Page 56, line 2. Support for newly added Claim 128 is found at least at Page 41, lines 4-6. Support for newly added Claim 129 is found at least on Page 33, lines 8-10. New Claims 126-129 are dependent on Claim 46, thus the forgoing arguments and distinctions over the prior art apply. Acceptance is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims (46-48, 50-72 and 125-129) are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By Caroline M Fleming

Caroline M. Fleming
Registration No. 45,566
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 7/13/04